CONFIDENTIAL

Attention: FTC Secretary, Mr. Don Clark
Fax: 202 326-2012

Dear Mr. Clark:

As a private citizen of the United States subjected to the abuse of power under color of law, I can attest to the uses and abuses of social security numbers by all manner of companies and organizations. The back of my social security card specifically states that it is not to be used for identification. Prior to 1970, a social security card was issued when a person turned 16 and wanted to get a part time job. The required documentation was a certified copy of the birth certificate and another form of identification along with a parent's signature. After I married and had children, the social security cards were issued at birth. My children were born in the 80's. At about the same time, social security numbers were required to get credit, to open savings, checking, investment accounts, to take college entrance exams, to get into colleges and schools and even to get bowling sanctions. I have consistently and repeatedly rebelled against the abuse and misuse of social security numbers indicating, to everyone who asked, that the card is not to be used for identification. At one point I looked up the laws regarding use of social security numbers and found a specific Federal statute that would cause the abuser to incur a $1200 fine per abuse. I carried a copy of that law with me for years and have only recently misplaced it. I would explain to everyone who asked for my social security number that I would gladly give it to them if they would pay me a salary or wages. The proper use of social security numbers is for the purpose of withholding payroll taxes, paying taxes and collecting social security benefits.

When I became a licensed insurance broker, the state licensing board demanded my social security number and had the audacity to use that number as my license number. I was required to write my license number on every insurance application I submitted and since a copy of the application is left with the client and another is included in every policy that's issued, my social security number became public record. I fought to get a separate and distinct license number, arguing the points mentioned above and I sent a copy of the law to the state-licensing bureau to let them know I was very serious. I did receive a separate number.

When I enrolled my children in school, the school demanded their social security numbers and refused to educate them if I didn't provide them to the school administration (This is grades K-12). Several months after the administration had gotten the social security numbers, we received mail from Harris Bank and numerous other companies with our children's social security numbers displayed prominently on mailing labels. I still have examples of those documents in a secure place and will provide them when you allow me to testify at the public hearings. I made a formal complaint to the school regarding violation of our rights to privacy and publication of private information and demanded that they cease and desist giving those numbers to outside parties. At the same time, the school contracted with a computer provider and decided that our children would use their social security numbers as their identification to get on the computers. I absolutely refused to allow this and had to threaten the school with a lawsuit to have them stop this abuse. After these problems, I refused to give our social security numbers and other

personal information to the school for any reason whatsoever and told them to sue me if they wanted but they had no right to our social security numbers. They had no right to distribute our private information without our written permission.

My husband was in the NAVY and his social security number was required to access the Navy bases and benefits. I refused to give my social security number to anyone because I believed the law demanded that it only be used for collection of social security taxes. As a result, my husband's social security number appeared on all my "dependent" identification information. I couldn't say much about the government's use of my husband's social security number because he was a government employee and I believed at the time that the government had a legal right to use the number.

When I went to get my driver's license in the State of Illinois, my social security number was prominently displayed on the front of the driver's license. Since the driver's license is the required form of identification for cashing checks, obtaining credit, verifying identification, etc. the clerks would try to write my social security number on the form (check, application for credit, whatever) and I would raise the roof. I walked out of the stores because they were so adamant about the collection of these numbers and it was only upon my walking out that they would relent and admit that they didn't need the number. I placed a piece of gold tape over my social security number on my driver's license and numerous people, including a law enforcement officer at one time) had the audacity to try to remove the tape. (I didn't permit that and told the officer if he wanted my social security number, he needed to get a warrant). When my driver's license was up for renewal, I demanded that the license facility not place my social security number on my license and I handed them a copy of the federal law. I will find chapter and verse of that law and be sure to bring it when I am permitted to testify regarding the use and abuse of social security numbers.

When I went to work for a credit union, the credit union was going to use my social security number as a computer security number. I refused to allow that and explained that the law did not permit this use of the social security number – that it was supposed to be for the collection and payment of taxes and social security benefits only. As it turned out, the computers were hacked one day and those who had allowed the use of their social security numbers were placed at risk.

When I go to the doctor, the doctor demands my social security number (which I refuse to give) and hospitals, pharmacists and all kinds of organizations demand my social security number. I refuse but many people don't. I also ask that anyone who might have a legitimate reason to have my social security number sign a statement that they will be responsible for the safekeeping and ensuring the privacy of all my personal information and that they may not release that information to anyone without my express written permission. If the company refuses to sign that statement, they don't get my social security number. For employers, I indicate that my personal information, including my social security number, is not to be released to anyone without my express written permission. Naturally, to enforce that document would require that I get proof that this was the offending company and would also require me to go through legal channels to regain my privacy. There are absolutely and unequivocally, no safeguards for the individual citizens and there is no recourse for the abuse of privacy except to file lawsuits which most of us cannot afford.

Before the credit bureaus took control of our private information, the requirements for checking credit were a signed release form for each and every company where a person had credit. If a person was applying for insurance, a release form was required for each policy, for each company, for checking of driver's records, criminal records, etc. That requirement kept the control of personal information in the hands of the individual. With the advent of the credit bureaus and blanket releases, the individual lost control of all his/her private information and the doors were opened wide for identity theft and abuse of private information. Even though the government claimed that we could audit our credit report and the credit bureaus would be required to correct erroneous information, the fact was that they did nothing to do so. A person would have to file a lawsuit to have information corrected. Meanwhile, the incorrect information would still be distributed by the credit bureaus. Their response to requests to investigate the misuse and incorrect information ALWAYS resulted in a letter that stated, "We have checked our information and found it to be correct." Despite copies of letters written to the credit card companies and demands that the credit bureaus not release any information to anyone without our notarized written permission, the credit bureaus took it upon themselves to release information to anyone who asked without checking their right to access that information. Furthermore, they did nothing to verify that the information they were giving out was factual and accurate.

Yes, we suffered identity theft before there was any help at all from law enforcement and we are still feeling the effects of it today. We place the full blame on the fact that the credit card companies and banks and other "data collectors" have outsourced our information without our permission to foreign countries. We add that the U.S. Government has failed to enforce the laws regarding personal information and has even failed to ensure that the information it collects is secure. Examples are the numbers of laptops that have been stolen that place taxpayers' data at risk. 4/5/07 "Thousands of taxpayers are potentially at risk of identity theft because the Internal Revenue Service has lost or experienced the theft of 490 laptops over the last three years, a government report concludes." "Release No. 0106.07 USDA Press Office, April 27, 2007" "USDA Narrows List to 63,000 Individuals Whose Private Data was Exposed". I have a stack of documentation regarding government's failure to protect our personal data, including a letter from the U.S. Navy regarding compromise of my husband's military records including his social security number.

Our most recent bout with misuse of social security numbers came as a result of our travel on business to Miami, Florida. We used a credit card to rent a car from Hertz. This was in January 2007. On our May 2007 statement, we received a $43.00 charge for a car rental in April in Miami, Florida. We were nowhere near Florida in April and called the credit card company immediately. To report the fraudulent use of the card, the company demanded our social security number, our mother's maiden name, and numerous other very private information. When I told my husband to ask where this "security person" was located, we were told that the person was in Manila, the Philippines. The person explained that they already had all the information and we just needed to verify it. We refused to give that information and we wrote a certified letter to the Credit Card Company President explaining the situation and that we needed some information about how U.S. law can be enforced on foreign soil. We also asked how our information could be secure from abuse and misuse and people who have no scruples and who

would sell the information to others for abuse and even identity theft. The President had no answers. The charge was removed but the problem has not been solved. The company demanded that we give them our social security number as a means of identifying ourselves and since the information was being transmitted to Manila, we refused.

When social security numbers are used by other than the government for identification, the government security is compromised. Until you think about how information is used and why it is used, you can never have a full understanding of the dangers associated with using social security numbers for identification purposes. We already know that illegal immigrants steal social security numbers and we know that terrorists covet social security numbers. Identity thieves consider social security numbers a veritable gold mine. Since the social security numbers are used by the Armed Forces to access bases and information, the opportunity for terrorists to get into secure areas via the use of stolen identification information is not only likely, it has occurred. When social security numbers are not verified for employees, our government is exposed to security leaks and organized crime is facilitated. Examples: When the unions (often associated with organized crime –remember Jimmy Hoffa) side with pro-illegal immigrant groups to stop the verification of social security numbers by getting an injunction, the government becomes an assistant, an accomplice, a facilitator for organized crime, illegal immigration, and violation of employment laws.

Think! What if some of the data available to foreign nations is for people whom security occupations like TSA, DOD, Justice, FBI, FAA, etc. Think of the potential to create a false identification that could be used in the worst scenario by terrorists or in a lesser degree by criminals for blackmail or fraud.

Each person should have his/her individual identity under control of that person. We need to get back to requirement of individual releases for information and we need to have people notified each and every time their credit information is accessed. The burden for assuring appropriate use of information and safeguarding of U.S. Citizens' personal data, indeed the security of our country is the most important job our government has to do. Therefore, the cost of ensuring that information is safeguarded and that people are immediately advised as regards anyone accessing their personal information should not even be a factor. That is a part of practicing proper safeguard procedures and ensuring that our country is secure. By instituting this notification practice immediately, I believe we will see an immediate reduction in identity theft because people would be aware of potential problems without having to be inconvenienced and pay fees to Credit Bureaus who should have no rights to hoarding our personal data. It would also require Credit Bureaus to ensure that the information they are giving out is not only authorized but that it is correct and true. This would be the first step in protecting our citizens. We need to have teeth in the law so that the individual has real recourse and real remedies for the abuse of their identity and the dissemination of incorrect information or unauthorized information by credit bureaus and other parties. We need to ensure that our private information cannot be outsourced out of the USA by credit card companies and data miners and other businesses and organizations. The penalties for allowing private information regarding citizens to be outsourced out of the country should be so significant that it would be considered treason and a capital crime. Identity theft is tantamount to a capital crime because it murders a person's good name,

their reputation, their ability to do business, their ability to get certain jobs, and so on. It murders their livelihood or severely disrupts it.

We are aware of several young people who found out that their identities were stolen when they applied for a mortgage. In one young man's instance, he was informed that he wouldn't qualify for a mortgage because he already had a house and a mortgage. He was sent bank statements that claimed he had $15,000 in savings (which he wished he had but really didn't). He was told he owned a very expensive car (which he did not) and as a result of applying for the mortgage, the IRS came after him for failure to pay taxes on the unclaimed income. He filed his tax returns based on his true identity and true employment and spent many months trying to get information from the IRS as regards where this alleged employment was supposed to have taken place, etc. As it turned out, the young man, in desperation, decided to use the $15,000 in savings that was credited to his name to pay the IRS and he was promptly arrested for using money that was not his. The identity thief was an illegal immigrant and got away free as a bird while our young friend spent time in jail. His life has been ruined while the illegal immigrant who stole his identity and caused him all this trouble is free to continue stealing and "committing financial murder" as well as "reputational murder". Not only is the illegal immigrant free but he is "protected" by a sanctuary city.

Failure of the government to enforce the laws of the land, to cross-reference and check social security numbers against employment records and employees is the main problem. When the government ignores the use of fraudulent social security numbers and collects social security based on those fraudulent numbers, it is contributing to the fraud and is also contributing to illegal acts and continuation of the abuse. It's also stealing from law-abiding citizens. It is contributing to organized crime and to invasion of the country by illegal immigrants who realize there is no penalty for breaking the laws when they are not enforced.

The federal judge who issued the injunction prohibiting the cross check of social security numbers and the sending out of miss-match letters is not only naïve but is facilitating abuse of power under color of law, contributing to organized crime and identity theft, is compromising Homeland Security and the Security of the country and is facilitating and promoting illegal immigration. The Judge has committed treason by failing to uphold the laws of the land and by promoting violations of Section 8, USC 1324 and 274A of the INA. The right to work in the USA is partially guaranteed by the use of social security numbers – that's why birth certificates and other verifiable information is required in order to obtain a social security number. The excuse by the judge that this violates a person's right to privacy is insane, especially since U.S. Citizens are required to give their social security numbers for numerous reasons and to provide identification in order to receive all types of services. To refuse to allow the cross-matching and sending out miss-match letters is facilitating the takeover of the USA by lawless groups and enterprises and promotes illegal immigration and gives labor unions unlimited power to abuse illegal immigrants and employers. For the ACLU and the AFLCIO to file that paperwork is self-serving and un-American and is in direct violation of Section 8, USC 1324A and 274A of the INA as well as the RICOH statutes and other laws.

No one can adequately address the life cycle of the SSN within the businesses and organizations that use it. The reason is that the information has been disseminated to so many different bodies

within and outside the organization that it would be impossible to know who has access to the data, where all the data is located, and what is being done with it. For example: Chase Bank out sources the information to Manila, Philippines. We have no idea how much access or control the Philippine government has over data collected there or where that data is stored or to where else it might have been transmitted. Since The Philippines is on the terror watch list (according to the government's own travel advisory website), can you imagine what terrorists can do with our social security information? They could literally bankrupt the country and could gain access to secure sites that would be integral to our own security – like military bases, airports, nuclear power plants, NASA, National Laboratories, Weapons plants, etc. How would the government know whether the person using the identification is the real owner or a terrorist? It is a matter of National Security to immediately get control of the social security numbers and ensure that information is verified and that people who are "stealing identities or using fraudulent numbers" are rounded up and punished to the fullest extent of the law. They are security risks. For no reason whatsoever should our private information be available to foreign corporations or foreign governments. We need to plug this leak immediately.

I believe I have answered most of the questions posed in the comment request. I can provide documentation and more information about the subject and I would be willing to serve on a Social Security task force to insure that every facet of this problem is addressed and that solutions are expedited.

As a bit of background, I have worked in retail, retail management, security data management, bookkeeping, banking and finance, am a FLMI and CLU and NASD registered representative, have worked in warehouses and numerous other kinds of business since I was 10 years old. I have attended our local Prosecutor's Academy and our Citizen Police Academy. I have served on local task forces for local issues. Therefore, I believe I have a broad based knowledge of how our social security numbers are used, how data is collected, and the abuses and potential for abuse that failure to enforce the laws promotes. I have solutions and would be happy to be a member of any task force that would work to resolve the issues.

If you have any questions or need to contact me, please feel free to do so.